

"Express Mail" mailing label number EV 327 137 147 US

Date of Deposit 10/26/03

Our File No. 9281-4674
Client Reference No. FC US02033

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
Takehito Sugawara)
Serial No. To Be Assigned)
Filing Date: Herewith)
For: Handling Device and Method of)
Security Data)

SUBMISSION OF CERTIFIED COPY OF PRIORITY DOCUMENT

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Transmitted herewith is a certified copy of priority document Japanese Patent Application No. 2002-301948 filed on October 16, 2002 for the above-named U.S. application.

Respectfully submitted,



Gustavo Siller, Jr.
Registration No. 32,305
Attorney for Applicant
Customer Number 00757

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 1 6 日
Date of Application:

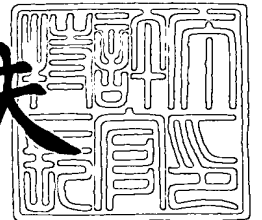
出 願 番 号 特 願 2 0 0 2 - 3 0 1 9 4 8
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 3 0 1 9 4 8]

出 願 人 アルプス電気株式会社
Applicant(s):

2 0 0 3 年 8 月 1 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 A7021

【提出日】 平成14年10月16日

【あて先】 特許庁長官殿

【国際特許分類】 E05B 49/00

【発明の名称】 セキュリティ関連データの取り扱い装置及びその取り扱い方法

【請求項の数】 5

【発明者】

【住所又は居所】 東京都大田区雪谷大塚町 1 番 7 号 アルプス電気株式会社内

【氏名】 菅原 健人

【特許出願人】

【識別番号】 000010098

【氏名又は名称】 アルプス電気株式会社

【代理人】

【識別番号】 100078134

【弁理士】

【氏名又は名称】 武 顕次郎

【電話番号】 03-3591-8550

【選任した代理人】

【識別番号】 100093492

【弁理士】

【氏名又は名称】 鈴木 市郎

【選任した代理人】

【識別番号】 100087354

【弁理士】

【氏名又は名称】 市村 裕宏

【選任した代理人】

【識別番号】 100099520

【弁理士】

【氏名又は名称】 小林 一夫

【手数料の表示】

【予納台帳番号】 006770

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0010414

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティ関連データの取り扱い装置及びその取り扱い方法

【特許請求の範囲】

【請求項 1】 携帯器認証部、不揮発性メモリ、制御部を有する車載器と、前記車載器、車載装置、通信部を有する車両と、前記通信部と通信して前記車両の車載装置の制御を指示する携帯器と、を備え、

前記車両のセキュリティに関連するデータを暗号キーを用いて暗号化する暗号化部を前記車載器の制御部と不揮発性メモリの間に介在させ、

前記制御部からの指示で前記セキュリティ関連データを前記暗号キーを用いて暗号化して前記不揮発性メモリに格納する

ことを特徴とするセキュリティ関連データの取り扱い装置。

【請求項 2】 請求項 1 において、

前記暗号キーは、前記セキュリティ関連データの暗号化信号を格納する前記不揮発性メモリとは別の不揮発性メモリに格納されることを特徴とするセキュリティ関連データの取り扱い装置。

【請求項 3】 請求項 2 において、

前記セキュリティ関連データは携帯器 ID を含み、前記不揮発性メモリは E E P R O M であり、前記別の不揮発性メモリは R O M であることを特徴とするセキュリティ関連データの取り扱い装置。

【請求項 4】 請求項 3 において、

前記 E E P R O M には前記携帯器 ID に加えて車載器 ID を格納することを特徴とするセキュリティ関連データの取り扱い装置。

【請求項 5】 携帯器認証部、不揮発性メモリ、制御部を有する車載器と、前記車載器、ドアロック機構、通信部を有する車両と、前記通信部と通信して前記車両のドアロック機構をロック又はアンロックさせる携帯器と、を備えて、前記車両のセキュリティに関連するデータの取り扱い方法であって、

前記車載器の制御部と不揮発性メモリの間に設けられた暗号化部で前記セキュリティ関連データを暗号キーを用いて暗号化し、

前記暗号化した暗号化信号を前記不揮発性メモリに格納するとともに、前記暗

号キーを前記不揮発性メモリとは別の不揮発性メモリに格納することを特徴とするセキュリティ関連データの取り扱い方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、携帯器との通信によって車両ドアのロック、アンロックを自動的に実行する際、リモートキーレスエントリ（RKE）におけるIDコード及び暗号キー等のセキュリティ関連データを取り扱う技術に関する。

【0002】

【従来の技術】

図3に、リモートキーレスエントリ（RKE）のブロック構成とIDコード及び暗号キー等のセキュリティ関連データの取り扱い方法を示す。図3において、車両1は、ドアロック機構5を有してそのドアの開閉を検出する検出部4を備えている。更に、車両1内には車載器2が設置され、車載器2は、携帯器20からのドアロック、アンロックの信号を携帯器送受信アンテナ3を通して携帯器認証部6で携帯器IDを認証し、認証の結果、ID合格ならばドアをロック、アンロックするように統括制御部7でドアロック機構を制御する。その際、EEPROM9にはID（車両ID、携帯器ID）及び暗号キー（携帯器と車両とは暗号キーによって暗号化された信号で通信する）を記憶し、ROM8には統括制御のためのプログラムを記憶する。

【0003】

従来、車両のドアロック機構をロックしたりアンロックするリモートキーレスエントリ（RKE）には、携帯器から車載器への一方向通信であるマニュアルRKEの他に、携帯器と車載器とで双方向通信を行うパッシブ（Passive）RKEが知られている。このパッシブRKEは、車両、例えば自動車のドアロックのロック、アンロックを自動的に行うもので、人間の携帯する携帯器と車両に搭載される車載器との間で双方向の通信を行い、携帯器IDや車両IDの認証の結果、正当な携帯器であることを車載器が確認したときにドアロック機構5に対してロック又はアンロックの動作を行う。この際、認証のために、携帯器及び車

載器は互いの認証を行うためにユニークなID (Identification Code ; 認証コード) と暗号キー (Key) を有し、それぞれの通信時には、IDを含むデータを暗号キーで暗号化した信号で通信する。

【0004】

パッシブRKEの具体的機能を説明すると、車載器2は一定周期毎にリクエスト信号を発信する。リクエスト信号には車載器IDが含まれ、比較的短い距離にしか到達しない。携帯器20がリクエスト信号の到達範囲外にあるときは携帯器はこのリクエスト信号を受信することはない。一方、携帯器を携帯する人間が自動車に接近し、リクエスト信号の到達範囲に至ると携帯器はリクエスト信号を受信し、リクエスト信号中の車載器IDをチェックし、それが正当な車載器から発せられたものであると認識すると、携帯器はレスポンス信号を発信する。

【0005】

車載器はレスポンス信号を受信し、その中に含まれる携帯器IDを取り出し、メモリに登録されている携帯器IDと前記レスポンス信号中の携帯器IDを照合し、一致したときは、ドアロック機構5に対して、アンロック信号を発信し、ドアロックをアンロック（解除）させる。照合が不成功に終わると、ロック機構に対して制御信号を発信しない。また、携帯器を持った人間が、車両から降りて離れるときには、携帯器がリクエスト信号を受信できなくなった時点で、つまり車載器がレスポンス信号を受信できなくなった時点で、車載器はドアロック機構に対してロック信号を発信する。

【0006】

リクエスト信号とレスポンス信号は、携帯器と車載器が共通に記憶している暗号化キーによって暗号化されて発信され、受信した側は、自己が記憶している暗号キーで信号を解読する。

【0007】

ID、暗号化キー等のセキュリティ関連データは、バッテリーを外されても記憶していなければならないため、EEPROMやROMなどの不揮発性メモリへ格納している。EEPROMやROMへ格納しているデータは固有データそのままの形式の情報値である。特に、車載器においては、携帯器IDが次に示すような

特殊事情のために、ROMではなくて、EEPROMに記憶される。そして、特殊事情とは、車載器においては最初から携帯器IDが記憶されているわけではなく、任意の携帯器（1台の車両に対してIDの異なる複数の携帯器）からのレスポンス信号を受けた車載器が、信号を分析し、その携帯器に予め記憶された携帯器IDを取り出して自己の不揮発性メモリに記憶することである。

【0008】

そして、この作業は、自動車ディーラやユーザが随時に行うことができるので、携帯器と車載器を製造工場でペアリング（対応付け）しなくても済むというメリットがある。しかし、上述したように後になってID登録するので、記憶媒体としてROMを用いることができない。更に、暗号キーも同様に、後になって、車載器と携帯器のいずれか一方から他方に送信された信号を介して他方に登録されるために（図3では携帯器にメモリが図示されていないが、携帯器にメモリがある）、ROMではなくEEPROMに記憶されている。

【0009】

【発明が解決しようとする課題】

上述した従来技術において、不揮発性メモリとしてのROMは、ROM内の記憶内容の解読を阻止する構造を採用しているので、解読するにしても多くの時間と手間を必要とする。これに対して、通常、EEPROMはその構造上ICの仕様にしたがえば記憶内容の解析が比較的容易である。したがって、EEPROMに記憶された携帯器IDや暗号キーのデータが他人に解読され、その規則性などが分析されてしまうと、多数の自動車のセキュリティが崩壊してしまうという事態に発展する虞が生じる。従来技術では、ID、暗号化キー等のセキュリティ関連データがそのままの値をEEPROMに格納して、自動車のセキュリティの観点で課題が生じていた。

【0010】

本発明の目的は、不揮発性メモリであるEEPROM及び／又はROMに格納しなければならないセキュリティ関連データを暗号化して格納することで、データを仮に読み取られても解読できないようにすることにある。

【0011】

【課題を解決するための手段】

前記課題を解決するために、本発明は次のような構成を採用する。

携帯器認証部、不揮発性メモリ、制御部を有する車載器と、前記車載器、車載装置、通信部を有する車両と、前記通信部と通信して前記車両の車載装置の制御を指示する携帯器と、を備え、前記車両のセキュリティに関連するデータを暗号キーを用いて暗号化する暗号化部を前記車載器の制御部と不揮発性メモリの間に介在させ、前記制御部からの指示で前記セキュリティ関連データを前記暗号キーを用いて暗号化して前記不揮発性メモリに格納するセキュリティ関連データの取り扱い装置。また、携帯器認証部、不揮発性メモリ、制御部を有する車載器と、前記車載器、ドアロック機構、通信部を有する車両と、前記通信部と通信して前記車両のドアロック機構をロック又はアンロックさせる携帯器と、を備えて、前記車両のセキュリティに関連するデータの取り扱い方法であって、前記車載器の制御部と不揮発性メモリの間に設けられた暗号化部で前記セキュリティ関連データを暗号キーを用いて暗号化し、前記暗号化した暗号化信号を前記不揮発性メモリに格納するとともに、前記暗号キーを前記不揮発性メモリとは別の不揮発性メモリに格納するセキュリティ関連データの取り扱い方法。このようなセキュリティ関連データの取り扱い装置又は方法によって、セキュリティ関連データを不揮発性メモリに保管するに際して暗号キーを用いて暗号化した信号形式で格納するので、車両のセキュリティ関連データを解読される虞はなくなる。

【0 0 1 2】

また、前記セキュリティ関連データの取り扱い装置において、前記暗号キーは、前記セキュリティ関連データの暗号化信号を格納する前記不揮発性メモリとは別の不揮発性メモリに格納される構成とした。更に、前記セキュリティ関連データの取り扱い装置において、前記セキュリティ関連データは携帯器 I D を含み、前記不揮発性メモリは E E P R O M であり、前記別の不揮発性メモリは R O M である構成とした。これらの構成によって、携帯器 I D などのセキュリティ関連データの取り扱いに際して、暗号キーは解読され難い R O M などの不揮発性メモリに記憶保管しておくので暗号キーが読み出される虞はなくなる。

【0 0 1 3】

【発明の実施の形態】

本発明の実施形態に関するセキュリティ関連データの取り扱い装置及び方法について、図1と図2を参照しながら説明する。図1は、本発明の実施形態に係る、リモートキーレスエントリにおけるIDコード及び暗号キー等のセキュリティ関連データの取り扱いシステムを示すブロック図であり、図2は、本実施形態に関する、セキュリティ関連データのEEPROMへの格納フローを示す図である。

【0014】

図面において、1は車両、2は車載器、3は携帯器送受信アンテナ、4はドア開閉検出部、5はドアロック機構（車載装置）、6は携帯器認証部、7は統括制御部、8はROM、9はEEPROM（Electrically Erasable Programmable Read-Only Memory）、10はデータ暗号化制御部、20は携帯器、21は携帯器アンテナ、22は携帯器内EEPROM、をそれぞれ表す。

【0015】

図1において、車両1と携帯器20とはパッシブキーレスエントリを構成しており、車載器2と携帯器20とで双方向通信を行ってドアロックのロック又はアンロックを自動実行するとともに車両の保安管理を厳重にしたキーレスエントリである。即ち、携帯器20が車載器2からのリクエスト信号の到達領域に入ると、携帯器20はリクエスト信号を受信することでレスポンス信号を発信し、車載器2はレスポンス信号を受信してID照合の結果、ドアロックを解除（アンロック）するようになっている。更に、携帯器20が車両1から離れるときは、車載器20が携帯器20からのレスポンス信号を受信できなくなったときにドアロック機構5に対してドアロックするように動作するものである。

【0016】

具体的に説明すると、車載器2から車載器IDを含んだリクエスト信号をアンテナ3を通して一定周期毎に携帯器20に送信し、一方、携帯器20からはアンテナ21を通して携帯器IDを含んだレスポンス信号を車載器2に送信して、双方向通信を行う。車載器2の携帯器認証部6において、携帯器20からのレスポ

ンス信号に含まれた携帯器IDと、予めEEPROM9に記憶されていた携帯器IDとを照合し、ID照合が一致したときは、統括制御部7はドアロック機構5にアンロック信号を発してドアロックを解除する。ID照合が一致しないときは統括制御部7はドアロック機構5にアンロック信号を発せず、ドアロックを解除しない。

【0017】

ここで、車載器2からのリクエスト信号及び携帯器20からのレスポンス信号は、携帯器と車載器が共に記憶している第1の暗号キーによって共に暗号化されて発信され、受信側では自己が記憶している第1の暗号キーでリクエスト信号又はレスポンス信号を解読するようになっている。

【0018】

また、リモートキーレスエントリ(RKE)を使用するに当たって、レスポンス信号に含まれる携帯器IDは、車載器をID登録モードに設定した後携帯器20から発せられたレスポンス信号を車載器で分析して各携帯器独自の携帯器IDを取り出してEEPROM9に記憶することにより新規に車載器に登録される。換言すると、車載器2には当初から予め規定された携帯器IDが記憶されている訳ではなく、携帯器の携帯器IDを学習して記憶している。このように、携帯器IDを車載器製造完了と同時にではなくて、RKEの使用開始前に記憶する必要があるために、携帯器IDは、不揮発性メモリの内でROMでなく、EEPROMに記憶する。

【0019】

図1における車両1のEEPROM9には、上述したように、当該車両に対する複数の携帯器に付された携帯器IDの他に、当該車両の車載器IDを格納している。ここで、複数の携帯器に対して、それぞれ異なるIDを付しても良いし、同一のIDを付しても良く、更に、グループ別に異なるIDを付しても良い。

【0020】

また、EEPROM9に記憶されるID(携帯器ID、車載器ID)は、データ暗号化制御部10によって第2の暗号キーによって暗号化された信号であり、これが、本発明の特徴の一つである。従来技術のようにIDをそのままの信号形

式でEEPROMに記憶すれば、EEPROMの構造上解読される虞があり、車両のセキュリティの観点で不安が生じる。本発明では、第2の暗号キーを用いてIDを暗号化してEEPROM9に記憶しているので、例え、そのデータを読み取られても解読はできないものである。そして、この第2の暗号キーは、リクエスト信号及びレスポンス信号に対する第1の暗号キーと共に、解読が難しいROM8に格納される。

【0021】

また、図2には、携帯器からのレスポンス信号に含まれる携帯器IDを取り出してEEPROMに記憶するフローを示している。統括制御部7からEEPROMへデータ（例えば、携帯器ID）を格納する指示が発生すると（ステップ1）、データ暗号化制御部10は、或る関数 $f_2(E-Key, data) = E-data$ を用いることによってセキュリティ関連データを暗号化させる（ステップ2）。ここで、 $f_2(x, y)$ は第2の暗号キーを用いた暗号化関数であり、 $E-Key$ はEEPROMへ格納するデータを暗号化させる暗号キーであり、 $data$ はEEPROMへ格納するセキュリティ関連データであり、 $E-data$ はEEPROM格納用に $data$ を暗号化したものである。また、或る関数 $f_2^{-1}(E-Key, E-data) = data$ を用いて暗号化データ復元させる。次に、ステップ3で暗号化データをEEPROMに格納する。

【0022】

以上説明したように、本発明によれば、車載器と携帯器との通信に使用するデータ（例えば、リクエスト信号、レスポンス信号）を第1の暗号キーによって暗号化するとともに、ROMではなくてEEPROMに格納すべきセキュリティ関連データ（例えば、ID）を第2の暗号キーによって暗号化して、解読をできなくさせるものであり、その際、第1の暗号キーと第2の暗号キーはともに解読が難しいROMに格納しておく。

【0023】

車載器のEEPROM9に携帯器IDを格納することを例示して説明したが、このEEPROM9には携帯器IDに加えて、車載器IDも格納されていて、この車載器IDも同様に第2の暗号キーで暗号化されている。また、携帯器20に

もEEPROM22や不図示の制御部を設けて、この不揮発性メモリに車載器IDや当該携帯器IDを暗号化して格納しても良い。

【0024】

また、一定周期毎にリクエスト信号を発信するパッシブRKEを例示して説明したが、トリガスイッチを例えばドアハンドルに設け、トリガスイッチを操作したときにリクエスト信号の発信が開始されるようにしても良い。更に、車載装置がドアロック機構であることを例示して説明したが、車載装置はこれに限定されず、例えばエンジン始動装置など他の装置であっても良い。エンジン始動装置の場合、トリガスイッチはメカニカルキーを挿入するイグニッションシリンダに内蔵されたり、又は単独のスイッチとしても良い。

【0025】

【発明の効果】

本発明によれば、セキュリティ関連データを不揮発性メモリに保管するに際して暗号キーを用いて暗号化した信号形式で格納するので、車両のセキュリティ関連データを解読される虞はなくなる。

【0026】

また、暗号キーは解読され難いROM等の不揮発性メモリに記憶保管しておくので暗号キーが読み出される虞はなくなる。

【0027】

更に、リモートキーレスエントリーにおけるリクエスト信号やレスポンス信号における通信に際しても他の暗号キーで暗号化して双方向通信することでセキュリティを確保すると共に、当該他の暗号キーも解読され難いROM等の不揮発性メモリに記憶保管しておくので当該他の暗号キーも読み出される虞はなくなる。

【図面の簡単な説明】

【図1】

本発明の実施形態に係る、リモートキーレスエントリーにおけるIDコード及び暗号キー等のセキュリティ関連データの取り扱いシステムを示すブロック図である。

【図2】

本実施形態に関する、セキュリティ関連データの E E P R O M への格納フローを示す図である。

【図 3】

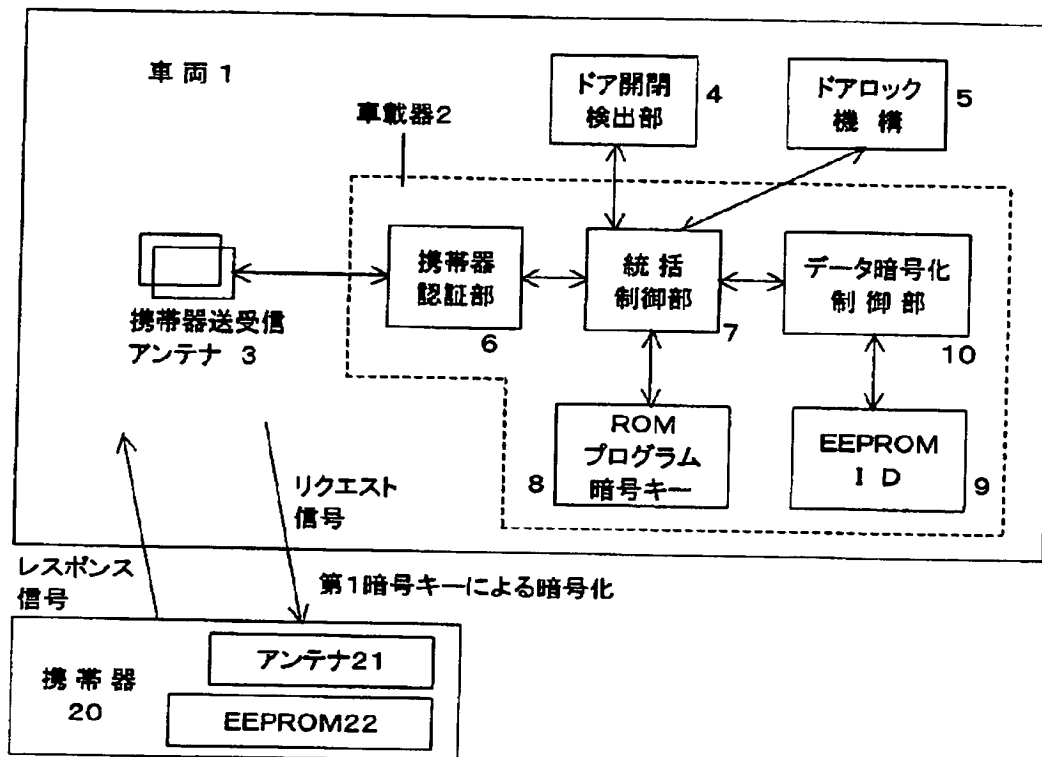
従来技術に関する、リモートキーレスエントリのブロック構成と I D コード及び暗号キー等のセキュリティ関連データの取り扱い方法を示す図である。

【符号の説明】

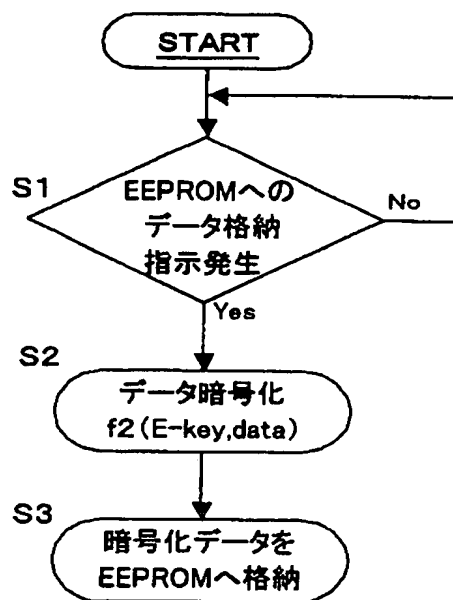
- 1 車両
- 2 車載器
- 3 携帯器送受信アンテナ
- 4 ドア開閉検出部
- 5 ドアロック機構（車載装置）
- 6 携帯器認証部
- 7 統括制御部
- 8 R O M
- 9 E E P R O M
- 1 0 データ暗号化制御部
- 2 0 携帯器
- 2 1 携帯器アンテナ
- 2 2 E E P R O M

【書類名】 図面

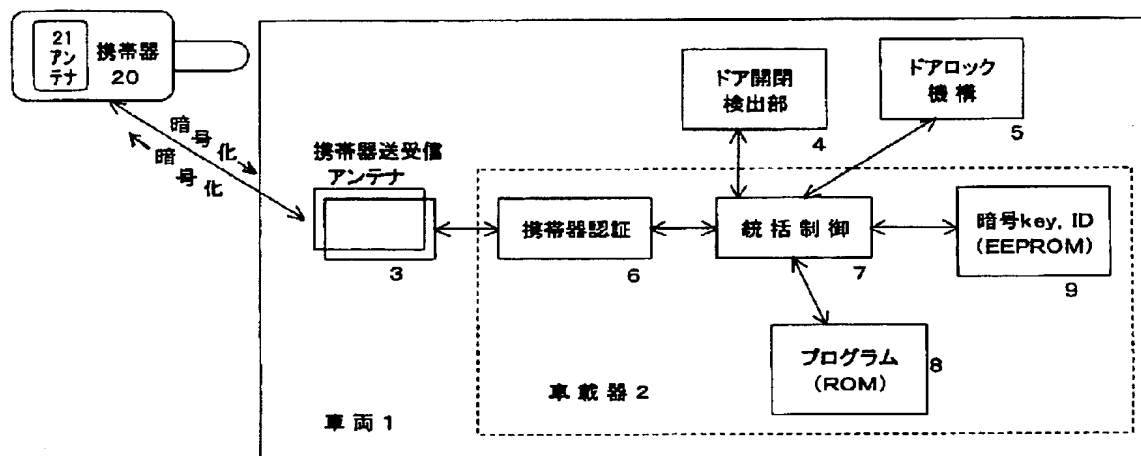
【図1】



【図 2】



【図 3】



【書類名】 要約書

【要約】

【課題】 不揮発性メモリに格納しなければならないセキュリティ関連データ（例えば、携帯器 I D）を暗号化して格納することで、データを仮に読み取られても解読できないようにすること。

【解決手段】 携帯器認証部 6、E E P R O M 9、R O M 8、制御部 7 を有する車載器 2 と、車載器 2、ドアロック機構 5、通信部 3 を有する車両 1 と、車両 1 のドアロック機構 5 をロック又はアンロックさせる携帯器 2 0 と、を備えて、車両のセキュリティに関連するデータ（例えば、携帯器 I D）を取り扱う装置において、セキュリティ関連データを暗号キーを用いて暗号化する暗号化部 1 0 を制御部と E E P R O M の間に介在させ、携帯器認証部の認証結果に基づいて制御部からの指示で携帯器 I D を暗号キーを用いて暗号化して E E P R O M 9 に格納するとともに、暗号キーは R O M 8 に格納すること。

【選択図】 図 1

特願 2 0 0 2 - 3 0 1 9 4 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 1 0 0 9 8]

1 . 変更年月日

1 9 9 0 年 8 月 2 7 日

[変更理由]

新規登録

住 所

東京都大田区雪谷大塚町 1 番 7 号

氏 名

アルプス電気株式会社